

## **IN THE CLAIMS**

This listing of the claim will replace all prior versions and listings of claim in the present application.

### **Listing of Claims**

Claims 1-7 (canceled).

8. (previously presented) An encryption apparatus comprising:  
a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of plaintext data to be encrypted; and

an operation section for conducting an exclusive OR-ing operation on the generated pseudorandom number sequence and the plaintext data, thereby calculating ciphertext data and outputting the ciphertext data,

wherein said pseudorandom number generating apparatus comprises:

a state storage section,

a buffer,

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation,

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock, and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

wherein said state storage section has a capacity of 3 blocks (where one block has  $n$  bits), and said buffer has a capacity of a plurality of blocks, and

wherein said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs, and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

9. (previously presented) A decryption apparatus comprising:

a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of ciphertext data, by using information for determining a random number sequence used when generating the ciphertext data to be decrypted; and

an operation section for conducting exclusive OR-ing operation on the generated pseudorandom number sequence and the ciphertext data, and thereby calculating plaintext data, and outputting the plaintext data,

wherein said pseudorandom number generating apparatus comprises:

a state storage section,

a buffer,

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation,

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock, and

a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section,

wherein said state storage section has a capacity of 3 blocks (where one block has  $n$  bits), and said buffer has a capacity of a plurality of blocks, and

wherein said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs, and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

Claims 11-19 (canceled).